Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2018

Matias Mäntyniemi

LÄÄKINNÄLLINEN OHJELMISTO PILVIPALVELUSSA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2018 | 28 sivua, 2 liitesivua

Matias Mäntyniemi

LÄÄKINNÄLLINEN OHJELMISTO PILVIPALVELUSSA

Tämän opinnäytetyön aiheena oli tutkia lääkinnällisen ohjelmiston siirtämistä pilvipalveluun sekä sen tuomia vaatimuksia. Työssä käytiin läpi lakeja, määräyksiä ja ohjeistuksia, jotka vaikuttavat lääkinnällisen ohjelmiston siirtämiseen pilvipalveluun Suomen ja Euroopan unionin alueella.

Työn tutkimusmenetelmänä käytettiin kirjallisuuskatsausta. Työ koostuu teoriaosuudesta, jossa käydään läpi pilviteknologian perusteet ja lääkinnällisten laitteiden vaatimukset sekä käytännön osuudesta, jossa analysoidaan lakeja ja säädöksiä ja niiden vaikutuksia lääkinnällisen ohjelmiston siirtämiseen pilvipalveluun.

Käytännön osuudessa analysoitiin toimeksiantajan kanssa valittuja aineistoja, joihin kuuluu Euroopan unionin yleinen tietosuoja-asetus, Valtiovarainministeriön tietoturvallisuuden johtoryhmän kehittämät VAHTI-ohjeet sekä Puolustusministeriön kehittämä viranomaisten auditointityökalu Katakri. Analyysin perusteella koottiin lista, johon kerättiin olennaisimmat vaatimukset lääkinnällisen ohjelmiston siirtämiselle pilvipalveluun. Vaikka organisaatio, joka käsittelee potilastietoja tai muita salassa pidettäviä tietoja, joutuu joka tapauksessa täyttämään suurimman osan aineistosta määrätyistä vaatimuksista, listan perusteella organisaatio voi tehdä alustavan arvioinnin ja suunnitelman pilvipalvelun tuomista lisävaatimuksista ja niiden täyttämisestä.

ASIASANAT:

pilvilaskenta, terveydenhuolto, tietoturva, tietosuoja, GDPR, VAHTI-ohjeet, Katakri

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information technology

2018 | 28 pages, 2 pages in appendices

Matias Mäntyniemi

MEDICAL SOFTWARE IN CLOUD SERVICE

The purpose of this thesis was to research the requirements and benefits of transferring medical software to a cloud service. The thesis goes through the laws and standards that affect medical software and their utilization with cloud technology in Finland and the European Union.

The chosen research method for this thesis is a literature review and the thesis consists of a theoretical chapter, which goes through the definition of cloud computing and the classification and requirements of medical devices and a practical chapter in which the chosen material is analyzed.

In the practical chapter the materials, which include the European Union's General Data Protection Regulation, the VAHTI-instructions of the cyber security executive team of the Ministry of Finance and Katakri, a security auditing tool developed by the Ministry of Defense. A list was made, based on the analysis, which includes the essential requirements for utilizing a cloud service with a medical software. Even though an organization that handles personal information of patients would already fulfill most of these requirements, the list is useful for the organization to determine the specific requirements of cloud services and medical software and form a rudimentary plan to fulfill them.

KEYWORDS:

Cloud computing, healthcare, information security, data protection, GDPR

SISÄLTÖ

1 JOHDANTO **6**

2 PILVITEKNOLOGIA **7**
2.1 Vastuu tietoturvallisuudesta 8
2.2 Hyödyt ja riskit 10

3 LÄÄKINNÄLISET LAITTEET JA OHJELMISTOT **11**

4 AINEISTON ANALYSOINTI **12**
4.1 GDPR 12
4.1.1 Tietojen käsittely 13
4.1.2 Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudet 14
4.1.3 Tietojen siirtäminen järjestelmästä toiseen 14
4.2 VAHTI-ohjeet 15
4.2.1 Sähköinen tietoturvallisuus 15
4.2.2 Salauskäytännöt 17
4.3 Katakri 18
4.3.1 Turvallisuusjohtaminen 18
4.3.2 Fyysinen turvallisuus 19
4.3.3 Tekninen tietoturvallisuus 20
4.3.4 Katakrin käyttö osana yritysturvallisuusselvitystä 21
4.4 Yhteenveto 22

5 JOHTOPÄÄTÖS **24**

LÄHTEET **25**

LIITTEET

Liite 1. Yhteenveto lääkinnällisten ohjelmiston vaatimuksista pilvipalvelussa.

KUVAT

Kuva 1. Turvallisuusselvitysprosessi 21

TAULUKOT

Taulukko 1. Vastuut pilvipalveluiden tietoturvasta 9
Taulukko 2. Yhteenveto lääkinnällisten ohjelmiston oleellisimmista vaatimuksista pilvipalvelussa 22

1 JOHDANTO

Pilviteknologia ja sen tuomat palvelut ovat yleistyneet viime vuosina paljon ja monet yritykset haluavat hyödyntää niiden tuomia mahdollisuuksia. Lääkinnälisia laitteita ja ohjelmistoja valmistavat ja potilas- ja henkilötietoja käsittelevät yritykset joutuvat ottamaan huomioon tietojen käsittelyyn ja säilyttämiseen liittyviä erityisvaatimuksia.

Tämän opinnäytetyön aiheena on selvittää, mitä tulee ottaa huomioon siirrettäessä lääkinnällistä ohjelmistoa pilvipalveluun. Työssä tutkitaan lakeja, määräyksiä ja ohjeistuksia, jotka saattavat vaikuttaa lääkinnällisten ohjelmistojen käsittelyyn. Työn tarkoituksena on selvittää, mitä lisävaatimuksia pilviteknologian käyttö tuo lääkinnälliselle ohjelmistolle sekä potilastietojen ja muiden salassa pidettävien tietojen käsittelylle.

Potilastietojen ja muiden salassa pidettävien tietojen käsittelyn ja säilyttämisen vaatimukset Suomessa on kuvattu esimerkiksi VAHTI-ohjeissa, Katakrissa sekä EU:n yleisessä tietosuoja-asetuksessa.

Työn tutkimusmenetelmänä käytetään kirjallisuuskatsausta. Työ koostuu teoriaosuudesta, jossa käydään läpi pilvilaskennan perusteet, pilvipalveluiden tietoturvan vastuut ja lääkinnällisten laitteiden vaatimukset sekä käytännön osuudesta, jossa analysoidaan EU:n yleisen tietosuoja-asetuksen, VAHTI-ohjeiden sekä Katakrin vaikutusta lääkinnällisen ohjelmiston siirtämiseen pilvipalveluun. Aineistot on valittu yhdessä toimeksiantajan kanssa.

2 PILVITEKNOLOGIA

Pilviteknologia on tietotekniikan laskennan malli, jossa laskenta tapahtuu hajautetusti ja joka mahdollistaa verkkoyhteyden yhteisiin ja konfiguroitaviin resursseihin esimerkiksi palvelimiin, tallennustilaan ja sovelluksiin (Mell & Grance 2011, 2). Pilvipalvelussa tiedot sijaitsevat organisaation ulkopuolella ja niitä käytetään internet-verkon ylitse (Valtiovarainministeriö 2015, 10). Resursseja voidaan jakaa ja julkaista nopeasti mahdollisimman vähäisellä vaivalla palvelun tarjoajalta. Pilvilaskenta jaetaan viiteen tärkeään piirteeseen, kolmeen palvelumalliin sekä neljään julkaisumalliin. (Mell & Grance 2011, 2.)

Pilvilaskennan historia ulottuu 1960-luvulle asti, jolloin tietotekniikan ala tunnisti laskennan tuottamisen palveluina tuomat hyödyt, vaikka varhaisilla tietokoneilla ja yhteyksillä ei riittänyt tehoa tähän. Vasta 1990-luvulla internetin laaja saatavuus mahdollisti laskennan tuottamisen palveluna. (Search Cloud Computing, 2017.)

Tärkeät piirteet:

1. *Vaadittava itsepalvelu.* Käyttäjä pystyy itse, tarpeen mukaan, varaamaan palveluita, kuten palvelinaikaa ja verkkotallennustilaa, ilman tarvetta asiakaspalvelulle
2. *Laaja verkkoyhteys.* Toiminnot ovat käytettävissä verkon kautta
3. *Resurssien yhdistäminen.* Palveluntarjoajan resurssit on yhdistetty palvellakseen useita käyttäjiä. Fyysiset ja virtuaaliset resurssit määrätään dynaamisesti ja uudelleen määrätään käyttäjien tarpeiden mukaan. Käyttäjällä ei yleensä ole valtaa tai tietoa resurssien tarkasta sijainnista.
4. *Nopea muuttuvuus.* Toiminnot voidaan dynaamisesti ja joissakin tapauksessa automaattisesti jakaa ja vapauttaa tarpeiden mukaan. Käyttäjälle resurssit usein näyttävät äärettömiltä.
5. *Mitattavat palvelut.* Pilvijärjestelmät mittaavat, ohjaavat ja optimoivat resursseja automaattisesti. Resurssien käyttöä voidaan valvoa, ohjata ja raportoida, tarjoten läpinäkyvyyttä sekä asiakkaalle, että palvelutarjoajalle.

(Mell & Grance 2011, 2.)

Palvelumallit:

1. *Software as a Service (SaaS).* Käyttäjälle tarjotaan mahdollisuus käyttää palveluntarjoajan ohjelmistoja, jotka pyörivät pilvi-infrastruktuurissa. Ohjelmistoja voi käyttää esimerkiksi verkkoselaimen tai ohjelmistorajapinnan kautta.
2. *Platform as a Service (PaaS).* Käyttäjälle tarjotaan mahdollisuus sijoittaa pilvipalveluun käyttäjän luomia tai hankkimia ohjelmistoja, jotka on luotu käyttäen palveluntarjoajan tarjoamia ohjelmointikieliä, kirjastoja, palveluja ja työkaluja.
3. *Infrastructure as a Service (IaaS).* Käyttäjälle tarjotaan mahdollisuus hyödyntää laskentaa, verkkoja, tallennustilaa ja muita tietotekniikkaresursseja, joissa käyttäjällä on mahdollisuus sijoittaa ja käyttää ohjelmistoja ja käyttöjärjestelmiä.

(Mell & Grance 2011, 2-3.)

Julkaisumallit:

1. *Yksityinen pilvi.* Pilvi-infrastruktuuri on jaettu käytettäväksi yhdelle organisaatiolle kattaen useita käyttäjiä.
2. *Yhteisöpilvi.* Pilvi-infrastruktuuri on jaettu käytettäväksi tietylle käyttäjäyhteisölle organisaatiosta, jolla on yhteisiä tehtäviä tai vaatimuksia.
3. *Julkinen pilvi.* Pilvi-infrastruktuuri on jaettu käytettäväksi julkisesti.
4. *Hybridipilvi.* Pilvi-infrastruktuuri on yhdistelmä kahta tai useampaa erilaista infrastruktuuria, jotka pysyvät erillisinä, mutta ovat yhteydessä teknologialla, joka mahdollistaa sovellusten ja tiedon siirrettävyyden.

(Mell & Grance 2011, 3.)

2.1 Vastuu tietoturvallisuudesta

Tietoturvallisuus on yksi organisaatioiden suurimpia huolenaiheita pilvipalveluiden kanssa. Varsinkin julkiset pilvipalvelut, jotka jakavat infrastruktuurinsa useiden asiakkaiden välillä, vaatii suuren erottelun eri asiakkaiden laskentaresurssien välillä. Monet organisaatiot, joita sitovat monet lait ja säädökset, ovat epävarmoja siirtämään tietojaan julkiseen pilveen katkosten, väärinkäytön ja varkauksien takia. Vastarinta on kuitenkin hiipumassa erottelun ja muiden tietoturvaratkaisujen osoittauduttua luotettaviksi. (Search Cloud Computing, 2017.)

Osana *IaaS*-palvelua palvelun tarjoajan tulee suojata kaikki ohjelmistot, alustat ja laitteet samalla tavalla kuin organisaation tiloissa sijaitseva infrastruktuuri. *PaaS*-palvelussa turvallisuus vaatimukset riippuvat paljolti siitä, mitä tietoja palvelussa käsitellään ja säilytetään. Turvallisuusratkaisu tulee järjestää tapaus kohtaisesti. *Saas*-palvelussa turvallisuus vaatimukset rajoittuvat käyttäjien käyttäytymiseen ja ohjelmiston käyttöliittymässä saatavilla oleviin asetuksiin. Vaikka palveluntarjoaja olisikin vastuussa turvallisuudesta, koska asiakkaan tiedot ovat vaarassa, asiakkaan täytyy varmistua palveluntarjoajan tietoturvasta. (Kulkarni 2016.)

Taulukko 1. Vastuut pilvipalveluiden tietoturvasta

Vastuu	Ohjelmisto palveluna (SaaS)	Alusta palveluna (PaaS)	Infrastruktuuri palveluna (IaaS)	Tiloissa sijaitseva
Tiedon hallinta	Asiakas	Asiakas	Asiakas	Asiakas
Päätelaite	Asiakas	Asiakas	Asiakas	Asiakas
Käyttäjien hallinta	Asiakas	Asiakas	Asiakas	Asiakas
Henkilöiden seuranta ja pääsy	Molemmat	Molemmat	Asiakas	Asiakas
Applikaatio	Palvelun tarjoaja	Molemmat	Asiakas	Asiakas
Verkon ohjaimet	Palvelun tarjoaja	Molemmat	Asiakas	Asiakas
Käyttöjärjestelmän turvallisuus	Palvelun tarjoaja	Palvelun tarjoaja	Asiakas	Asiakas
Isäntä palvelut	Palvelun tarjoaja	Palvelun tarjoaja	Palvelun tarjoaja	Asiakas
Verkko	Palvelun tarjoaja	Palvelun tarjoaja	Palvelun tarjoaja	Asiakas
Data keskus	Palvelun tarjoaja	Palvelun tarjoaja	Palvelun tarjoaja	Asiakas
Fyysisen turvallisuus	Palvelun tarjoaja	Palvelun tarjoaja	Palvelun tarjoaja	Asiakas

Taulukkoon 1 on koottu palveluntarjoajan ja asiakkaan vastuut eri pilvipalvelumallien tietoturvasta (Kulkarni 2016).

Asiakkaat kokevat pilvipalveluiden suurimmaksi hyödyksi fyysisen ympäristön vastuun siirtämisen palvelun tarjoajalle. Palvelun tarjoajilla on turvallisuus prosessit ja ohjeistukset, jotka auttavat varmistamaan luvattoman pääsyn tiloihin. (Simorjay 2017, 9.)

Yrityksen tiloissa sijaitsevissa ratkaisuissa, yritys on itse vastuussa omasta tietoturvastaan. *IaaS*-palvelussa rakennukset, palvelimet ja verkkolaitteet ovat palveluntarjoajan vastuulla. Asiakas on vastuussa ohjelmistoista, verkkoasetuksista ja henkilöiden hallinnasta. *PaaS*-palvelussa palveluntarjoaja on lisäksi vastuussa verkko ohjainten hallinasta ja turvallisuudesta. *SaaS*-palvelussa palveluntarjoaja tarjoaa myös itse ohjelmiston.

Asiakas on vastuussa tietojen asianmukaisesta salauksesta ja luokituksesta ja ne jakavat vastuun palveluntarjoajan kanssa henkilöiden seurannasta. (Simorjay 2017, 10.)

2.2 Hyödyt ja riskit

Pilviteknologia tarjoaa yrityksille paljon hyötyjä, mutta sen käyttöön liittyy sekä samoja riskejä, kuin mihin tahansa ulkoiseen palvelun tarjoajaan, että pilvipalveluille uniikkeja riskejä. Turvallisuuden ja riskienhallinnan näkökulmasta pilvipalvelu on yksi vähiten läpinäkyvistä ratkaisuista. Tietoja säilytetään ja käsitellään ulkoisesti useammassa eimääritellyissä tiloissa, jotka on usein hankittu ei-nimetyiltä palvelun tarjoajilta. (Heiser & Nicolett 2008, 2.)

Pilviteknologian hyötyjä ovat esimerkiksi IT-kulujen vähentyminen, kun yrityksen ei tarvitse maksaa laitteiston hankinnasta ja ylläpidosta tai kalliiden asiantuntijoiden palkkaamisesta. Yksi pilvi laskennan tärkeimpiä piirteitä on sen helppo skaalattavuus ja muokattavuus, joka yrityksellä tarkoittaa sitä, että palvelun tyyppiä ja hintaa voidaan nostaa tai laskea sen hetkisten tarpeiden mukaan. Liiketoiminnan jatkuvuuden varmistamiseksi pilviteknologia antaa mahdollisuudet helppoon ja nopeaan varmuuskopiointiin ja poikkeustilanteista palautumiseen. (Businnes Queensland 2017.)

Myös organisaation yhteistyö helpottuu, kun tarpeellista tietoa voidaan jakaa helposti eri sijaintien, toimistojen ja henkilöstön välillä. Palvelun tyypistä riippuen tietoja voidaan jakaa helposti myös organisaation ulkopuolella. Pilvipalvelu antaa myös henkilöstölle mahdollisuuden mukauttaa työskentelytapojaan tarpeen mukaan. (Businnes Queensland 2017.)

Pilviteknologia tuo myös mukanaan riskejä, joista suurimpia ovat tietoturvallisuus ja tietojen fyysinen sijainti. Yrityksen tulee varmistua palveluntarjoajan luotettavuudesta ja turvallisuudesta. Myös jotkut lait saattavat vaikuttaa esimerkiksi siihen, missä maissa tietoja saa säilyttää. (Businnes Queensland 2016.)

3 LÄÄKINNÄLISET LAITTEET JA OHJELMISTOT

Lääkinnällisellä laitteella tarkoitetaan laitteistoa, ohjelmistoa, välinettä tai materiaalia, jotka niiden valmistaja on yksinään tai yhdistelmänä tarkoittanut käytettäväksi seuraaviin asioihin:

1. ihmisen sairauden diagnosointiin, ehkäisyyn, tarkkailuun, hoitoon tai lievitykseen
2. vamman tai vajavuuden diagnosointiin, tarkkailuun, hoitoon, lievitykseen tai kompensointiin
3. anatomian tai fysiologisen toiminnan tutkimiseen, korvaamiseen tai muunteluun
4. hedelmöityksen säätelyyn. (Valvira 2017.)

Tuotteen valmistajan on annettava tuotteelleen terveydenhuollon laitteen ja tarvikkeen määritelmän mukainen käyttötarkoitus (Valvira 2009). Laitteet jaetaan luokkiin I, IIa, IIb ja III laitteen käyttötarkoituksen ja käyttöön liittyvien riskien perusteella. Jos laitteeseen sovelletaan useampia sääntöjä, sen käyttötarkoituksen perusteella laite luokitellaan ylimpään luokkaan. Laitteen toimintaan vaikuttava tietokoneohjelma kuuluu automaattisesti samaan luokkaan. (Neuvoston direktiivi 1993, 9, 58.)

4 AINEISTON ANALYSOINTI

Tässä luvussa analysoidaan Suomen ja EU:n lakeja, jotka saattavat vaikuttaa lääkinnällisten ohjelmistojen käyttöön sekä potilastietojen ja muun salassa pidettävän tiedon säilyttämiseen ja käsittelyyn pilvipalvelussa. Tutkimusmenetelmäksi valittiin kirjallisuuskatsaus jo olemassa olevan aineiston määrän ja laadun vuoksi. Aineistot on valittu yhdessä toimeksiantajan kanssa. Luvun lopussa on yhteenveto, johon on kerätty taulukkoon oleellisimmat vaatimukset aineistosta.

4.1 GDPR

General Data Protection Regulation (GDPR) on Euroopan Parlamentin ja Neuvoston vuonna 2016 antama asetus henkilötietojen käsittelystä ja näiden tietojen vapaasta liikkuvuudesta. Asetus astuu voimaan 25. toukokuuta 2018 kahden vuoden siirtymäajan jälkeen. (Tietosuojavaltuutetun toimisto 2015.) Euroopan parlamentti ja Euroopan Unionin neuvosto katsovat, että jokaisella on oikeus henkilötietojensa suojaan, heidän kansalaisuudestaan ja asuinpaikastaan riippumatta. EU:n yleisen tietosuoja-asetuksen tarkoituksena on yhdenmukaistaa henkilötietojen käsittelyä koskevien perusoikeuksien ja -vapauksien suojelua ja varmistaa henkilötietojen vapaa liikkuvuus jäsenmaiden välillä. (Euroopan parlamentin ja neuvoston asetus 2016, 1-2.)

Rajat ylittävä henkilötietojen siirto on lisääntynyt huomattavasti taloudellisen ja sosiaalisen yhdistymisen seurauksena. EU:n jäsenvaltioiden viranomaisia on kehotettu toimimaan yhteistyössä, jotta ne voisivat täyttää velvollisuutensa tai suorittaa tehtäviä jonkin muun jäsenvaltion viranomaisten puolesta. Asetuksen tulee koskettaa kaikkia henkilöitä heidän asuinpaikastaan ja kansalaisuudestaan riippumatta. (Euroopan parlamentin ja neuvoston asetus 2016, 2-3.)

Globalisaatio sekä teknologian kehitys tuovat henkilötietojen suojeluun uusia haasteita. Tämän kehityksen vuoksi Euroopan Unionissa tarvitaan vahva ja johdonmukainen tietosuojakehys, jota tuetaan tehokkaasti. Henkilöiden on voitava valvoa omia henkilötietojaan ja niiden liikkumista ja käyttöä. Henkilöiden oikeuksien ja vapauksien suojelun tason heidän henkilötietojensa käsittelyn ja liikkuvuuden kannalta tulee olla vastaava kaikissa jäsenvaltioissa. Väärinkäytön riskin välttämiseksi henkilöiden suojelun tulisi olla käytetystä teknologiasta riippumatonta. (Euroopan parlamentin ja neuvoston asetus 2016, 2.)

Asetuksen tarkoituksena on vahvistaa säännöt henkilöiden suojelulle henkilötietojen käsitellyssä ja tietojen vapaassa liikkuvuudessa. Asetus suojelee henkilöiden vapauksia ja oikeuksia henkilötietoihin ja henkilötietosuojaan liittyen. Henkilötietojen vapaata liikkuvuutta EU:n sisällä ei saa kieltää tai rajoittaa henkilöiden suojeluun henkilötietojen käsittelyssä liittyvistä syistä. (Euroopan parlamentin ja neuvoston asetus 2016, 5-6.)

4.1.1 Tietojen käsittely

Henkilötietojen käsittelyn tulee olla asianmukaista ja laillista. Henkilöille tulee läpinäkyvästi kertoa, miten heidän tietojaan kerätään ja käytetään. Tietojen käsittelyn tarkoitukset on määritettävä ja ilmoitettava kyseiselle henkilölle tietojen keruun yhteydessä. Läpinäkyvyyden periaatteen mukaan henkilötietojen käsittelyyn liittyvien tietojen tulee olla helposti saatavilla ja ymmärrettävissä. Henkilöille on kerrottava tietojen käsittelyyn liittyvistä riskeistä, säännöistä ja oikeuksista sekä opastaa miten he voivat hyödyntää käsittelyyn liittyviä oikeuksiaan. Rekisterinpitäjän tulee viipymättä ilmoittaa henkilötietojen tietoturvaloukkauksesta kyseiselle henkilölle. Ilmoituksessa tulee kuvata tietoturvaloukkauksen luonne ja suositeltava toimenpiteitä, joiden avulla asianomainen voi toteuttaa tarvittavat varotoimet ja lieventää tietoturvaloukkauksen mahdollisia haittoja. (Euroopan parlamentin ja neuvoston asetus, 2016 7-17.)

Henkilön tulee antaa suostumus selkeästi suostumusta ilmaisevalla toimella, esimerkiksi kirjallisesti tai suullisesti, josta käy ilmi henkilön vapaaehtoinen ja yksiselitteinen suostumus, jolla henkilö hyväksyy henkilötietojensa käsittelyn. Suostumuksen tulee kattaa kaikki käsittelytoimet. Jos rekisteröidyn on annettava suostumus sähköisesti, on pyynnön oltava tiiviisti ja selkeästi esitetty, eikä se saa häiritä palvelun normaalia käyttöä. Rekisterinpitäjän on voitava osoittaa rekisteröidyn antama suostumus. Jos suostumus annettaan jotakin muuta koskevan ilmoituksen yhteydessä, tulee varmistaa, että henkilö on tietoinen antamastaan suostumuksesta ja siitä mitä suostumus kattaa. (Euroopan parlamentin ja neuvoston asetus 2016, 5-6.)

Henkilöllä on aina oikeus vaatia rekisterinpitäjää korjaamaan henkilöä koskevat virheelliset ja epätarkat tiedot. Henkilöllä on myös oikeus vaatia rekisterinpitäjää poistamaan häntä koskevat tiedot, jos henkilötietoja ei enää tarvita tarkoituksiin joita varten ne kerättiin, henkilö poistaa suostumuksensa eikä käsittelyyn ole muita laillisia perusteita tai jos henkilötietoja on käsitelty lainvastaisesti. (Euroopan parlamentin ja neuvoston asetus, 2016 43-44.)

4.1.2 Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudet

Rekisterinpitäjän on suunniteltava ja toteutettava tarvittavat toimenpiteet, joilla varmistetaan, että tietojen käsittelyssä noudatetaan tätä asetusta. Toimenpiteet on tarkistettava ja päivitettävä tarpeen mukaan. Rekisterinpitäjän tulee myös toteuttaa asianmukaiset tietosuojaa koskevat toimintaperiaatteet sekä tarvittavat suojatoimet, jotta käsittely vastaisi asetuksen asettamia vaatimuksia ja henkilön oikeudet suojattaisiin. (Euroopan parlamentin ja neuvoston asetus 2016, 47-48.)

Henkilötietojen käsittelijöinä tulee käyttää ainoastaan sellaisia henkilöitä, jotka pystyvät toteuttamaan riittävät suojatoimet teknisten ja hallinnollisten toimien täytäntöönpanemiseksi niin, että käsittely täyttää tämän asetuksen vaatimukset ja varmistaa henkilöiden oikeuksien suojauksen. Käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluksia ilman erillistä kirjallista lupaa rekisterinpitäjältä. Tietojen käsittely on määritettävä sopimuksella tai muulla oikeudellisella asiakirjalla, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa määritellään käsittelyn kohde, kesto ja tarkoitus. Sopimuksessa on säädettävä erityisesti se, että henkilötietojen käsittelijä käsittelee tietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti ja sitoutuu noudattamaan salassapitovelvollisuutta. (Euroopan parlamentin ja neuvoston asetus 2016, 49.)

4.1.3 Tietojen siirtäminen järjestelmästä toiseen

Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot jäsennellyssä muodossa ja tallentaa ne henkilökohtaista käyttöä varten sekä siirtää kyseiset tiedot toiselle rekisterinpitäjälle. Yleisen tietosuoja-asetuksen tarkoitus on säädellä henkilötietoja, vaikka oikeus henkilötietojen siirtämiseen saattaakin lisätä palveluiden välistä kilpailua. Asetuksessa myös kielletään rekisterinpitäjää estämästä tietojen siirtämistä. (Tietosuojatyöryhmä 2016, 3-5.)

Tietojen siirtäminen ei saa rajoittaa henkilön muita oikeuksia. Rekisteröidyn tulee voida edelleen käyttää rekisterinpitäjän palveluita tietojen siirto-operaation jälkeen niin kauan kuin rekisterinpitäjä käsittelee tietoja. Tietojen siirtäminen ei automaattisesti tarkoita tietojen poistamista. (Tietosuojatyöryhmä 2016, 6-8.)

4.2 VAHTI-ohjeet

VAHTI on julkisen hallinnon digitaalisen turvallisuuden johtoryhmä, jonka valtiovarainministeriö on asettanut toimimaan hallinnon digitaalisen turvallisuuden kehittämisen ja ohjauksesta vastaavien organisaatioiden yhteistyö-, vastuu- ja koordinaatioelimenä. VAHTI kehittää myös ohjeistusta, joka kattaa tietoturvallisuuden kaikki osa-alueet. (Valtiovarainministeriö)

4.2.1 Sähköinen tietoturvallisuus

Sähköisellä asiointipalvelulla tarkoitetaan VAHTI-ohjeessa verkkopalvelua, jossa asiakas voi asioida viranomaisen kanssa tietoverkon avulla. Palvelun asiakkaita voivat olla kansalaiset, yritysten edustajat, viranomaiset tai tietojärjestelmät, jotka käyttävät asiointipalvelua teknisen rajapinnan kautta. Asiointipalveluun liitettävien taustapalveluiden ja tietojärjestelmien turvallisuudesta vastaa kyseisen palvelun omistaja. Omistaja on myös vastuussa palveluiden tietoturvallisen käytön ohjeistamisesta. (Rousku 2017, 19-22.)

Sähköisen asioinnin tietoturvariskeihin voidaan varautua jo suunnitteluvaiheessa rajaamalla tietojen käsittely asiointipalvelussa tiettyyn tietojoukkoon sen käyttötarkoituksen perusteella. Palvelun omistajan on myös suositeltavaa määrittää tietoturvalliset toimintatavat niin henkilökunnalle kuin palvelun asiakkaille. (Rousku 2017, 27.)

Palvelun omistajan tulee määrittää palvelussa käsiteltävän salassa pidettävän tiedon käsittelyperiaatteet erityisesti tiedon suojaamiselle asiointipalvelun sovellusympäristössä, palvelun ja taustajärjestelmien tiedonvaihdolle, tiedonvaihdolle toisen viranomaisen tai organisaation kanssa ja tiedon käsittelylle ei-luotetussa ympäristössä, kuten pilvipalvelussa tai asiakkaiden päätelaitteilla. (Rousku 2017, 28.)

Omistajan tulee myös tunnistaa palvelun keskeisimmät käyttötilanteet ja liittymät, joiden kautta palvelua käytetään. Omistajan tulee myös tunnistaa missä laajuudessa ja missä tietoverkoissa salassa pidettävää tietoa käsitellään. Erityistä huomiota vaativat usean organisaation käyttötilanteet, joissa salassa pidettävää tietoa luovutetaan muille osapuolille. (Rousku 2017, 28.)

Asiointipalvelun omistajan tulee myös arvioida palveluun kohdistuvia uhkia ja niiden vaikutuksia sekä varmistaa riittävä tietoturvan taso ja vaatimuksenmukaisuus. Riskien arvioinnin uusiminen on tarpeellista erityisesti, jos palvelussa käsiteltävä tietoaineisto muuttuu olennaisesti tai palveluun lisätään uusia toimintoja tai rajapintoja. Arvioinnissa tulee huomioida sekä ulkoiset että sisäiset riskit ja ottaa myös huomioon tahallinen väärinkäyttö ja väärinkäytön mahdolliset motiivit. Omistajan tulee myös säännöllisesti arvioida ja todentaa tietoturvallisuuden riittävä taso koko palvelutuotantoketjussa. (Rousku 2017, 28-31.)

Tietoturvallisuutta koskeviin tehtäviin tulee nimetä vastuuhenkilö. Tietoturvallisuuden kannalta tärkeitä tehtäviä ovat erityisesti poikkeustilanteiden käsittelyn johtamis- ja menettelytavat sekä salassa pidettävän tiedon käsittelysäännöt ja -käytännöt. Vastuuhenkilön vastuulla on suojata palvelun tekniset ympäristöt uhka-arvioinnissa tunnistetuilta tietoturvauhilta. Ympäristön ja henkilöstön altistuminen haittaohjelmille ja tietojen kalastelulle tulee minimoida. (Rousku 2017, 29-31.)

Palvelun omistajan tulee tarjota palvelun käyttäjille riittävän kattavat ohjeet ja tukipalvelut palvelun turvallista käyttöä varten. Erityisesti tunnistusvälineiden käyttöön, päätelaitteiden suojaamiseen haitallisilta ohjelmilta sekä asiointipalvelun turvalliseen käyttöön tulee ohjeistaa. (Rousku 2017, 29.)

Palvelun suunnittelussa tulee soveltaa ratkaisuja, jotka rajaavat pääsyä salassa pidettäviin tietoihin käyttäjien tarpeiden mukaan. Ratkaisut eivät kuitenkaan saa tarpeettomasti haitata tietojen tarpeenmukaista saatavuutta ja käsittelyä. Tietoon pääsyä tulee rajata rakenteellisesti esimerkiksi eriyttämällä ylläpitotoiminnot julkisista asiakaskäyttöliittymistä. Palvelussa tulee käyttää vain tietoturvallisiksi todennettuja ohjelmistoja ja tietorakenteita. (Rousku 2017, 30.)

Tietoturvasta huolimatta on mahdollista, että palvelu joutuu väärinkäytön kohteeksi. Palvelun omistajalla tulee olla valmiudet havaita ja käsitellä normaalista toiminnasta poikkeava tilanne. Riittävän kattavat lokitiedot palvelun tapahtumista ovat välttämättömät tietoturvan valvonnalle, poikkeustilanteiden havaitsemiselle sekä niiden selvitykselle. Jo suunnitteluvaiheessa tulee varmistaa, että palvelun tapahtumista kerätään riittävät lokitiedot ja että lokitiedot ovat tarvittaessa palvelun omistajan saatavilla. Kun palvelun normaalit käyttötilanteet ovat tiedossa, myös poikkeustilanteiden tunnistaminen ja käsittely on mahdollista. Tietoturvapoikkeamiin ja niistä palautumiseen tulee varautua etukäteen.

Poikkeamien käsittely ja niistä palautuminen vaatii eri osapuolten tehokasta yhteistoimintaa. Varautumisessa oleellisia asioita ovat varajärjestelmät ja –järjestelyt, jotka mahdollistavat asiakkaan asioinnin esimerkiksi palvelupisteissä ja toipumis- ja –viestintäsuunnitelmat palvelukatkojen ja tietoturvapoikkeustilanteiden varalle. (Rousku 2017, 32.)

4.2.2 Salauskäytännöt

Hyvä esimerkki salaustarpeesta on pilvipalvelu, jossa salassa pidettävä tieto sijaitsee organisaation ulkopuolella, mahdollisesti ulkomailla, ja jota käytetään internet-verkon ylitse. Pilviteknologia tuo uusia ja helpommin saatavilla olevia hyökkäystapoja esimerkiksi salasanojen murtamiseen. Pilvipalveluiden käyttöä voidaan laajentaa vasta, kun niissä on mahdollista käyttää asiakkaan tarkastamaa ja hyväksymää salausratkaisua. (VM 2015, 10-11.)

Salauksen kanssa tulee hyödyntää riskienhallintaa ja ottaa huomioon lakisääteiset ja liike- ja ydintoiminnan vaatimukset, sekä mahdolliset haasteet, joita käytettävä salaus tuo. Tietojen salaus tulee ottaa huomioon myös organisaation arkkitehtuurin suunnittelussa ja toteutuksessa, jotta organisaation pystyy hyödyntämään salausteknologiaa osana arkkitehtuurinsa kehittämistä. Salauksen avaintenhallinta tulee toteuttaa siten, että se täyttää kaikki asiakkaan vaatimukset. (VM 2015, 10.)

Organisaation tulee luokitella käsittelemänsä tiedot oikeaoppisesti. Tietojen yliluokittelu aiheuttaa ylimääräisiä kustannuksia ja aliluokittelu vaarantaa tiedon luottamuksellisuuden. Tiedot tulee salata tarpeen mukaan. Erityistä huolellisuutta on noudatettava kansainvälisten salassa pidettävien tietojen kanssa. Käytettävän salausratkaisun tulee täyttää määritetyt tarpeet ja vaatimukset. Salausratkaisu ei sellaisenaan riitä, vaan se tulee ottaa käyttöön oikeaoppisesti. Avaintenhallinta tulee myös suunnitella ja toteuttaa oikeaoppisesti. Salausjärjestelmien varmenteet tulee uusia hyvissä ajoin ennen niiden vanhenemista. Varmenteiden vaatimat toimenpiteet tulee vastuuttaa ja niiden hallitsemiseksi määrittää prosessit. Organisaation tulee salata kaikki kiintolevynsä. Koko turvallisuuskokonaisuus tulee auditoida ja testata säännöllisesti. Organisaatio on itse vastuussa omistamistaan tiedoista ja tietojärjestelmistä, vaikka niiden toteuttamisesta vastaisikin, jokin ulkopuolinen taho. (VM 2015, 17-18.)

4.3 Katakri

Katakri eli turvallisuusauditointikriteeristö on auditointityökalu, jota voidaan käyttää arvioitaessa sekä yritysten että viranomaisten turvallisuusjärjestelyjen toteutumista sekä tietojärjestelmien turvallisuuden arvioinneissa. Ensimmäinen Katakri valmistui puolustusministeriön, viranomaisten ja Elinkeinoelämän keskusliiton yhteistyössä vuonna 2009 osana hallituksen sisäisen turvallisuuden ohjelmaa. Koska yksittäisiin hankkeisiin voi sisältyä muutakin kuin Katakriin koottuja tiedon käsittelyä koskevia vaatimuksia, näiden vaatimusten toteutumista ei voi arvioida Katakrin avulla, joten tarkat turvallisuusvaatimukset tulee määrittää erikseen ottaen huomioon hankkeen erityistarpeet. (Katakri 2015, 3.)

Katakri on jaettu kolmeen osa-alueeseen: turvallisuusjohtamiseen, fyysinen turvallisuusteen sekä tekniseen tietoturvallisuuteen (Katakri 2015, 3).

4.3.1 Turvallisuusjohtaminen

Turvallisuusjohtaminen käsittää menetelmät, joilla turvallisuus ja sen hallinta otetaan osaksi koko organisaation toimintaa. Osa-alue kattaa hallinnollisen turvallisuuden ja henkilöturvallisuuden. Turvallisuusjohtamisen vaatimuksilla pyritään siihen, että organisaation turvallisuudenhallintajärjestelmä on toimiva ja riittävät menettelyt salassa pidettävien tietojen asianmukaisen käsittelyn varmistamiseksi. (Katakri 2015, 5.)

Turvallisuusjohtamisen vaatimuksiin kuuluu muun muassa se, että organisaatiolla on turvallisuusperiaatteet, jotka ovat organisaation ja suojattavien kohteiden kannalta tarkoituksenmukaiset ja kattavat. Turvallisuusperiaatteiden toteutumista tulee myös seurata ja raportoida. Organisaation tulee myös määritellä turvallisuuteen liittyvät tehtävät ja näille tehtäville vastuuhenkilöt. (Katakri 2015, 6-7.)

Vaatimuksiin kuuluu myös riskienhallintaprosessi, jonka tulee olla jatkuva ja säännöllinen. Riskienhallinnan on katettava vähintään turvallisuusjohtamisen sekä tila- ja tietoturvallisuuden osa-alueet. Riskienhallintaprosessia ja sen tuloksia hyödynnetään turvatoimien mitoituksessa, ottaen huomioon tiedon suojaustaso, määrä ja tyyppi. Organisaation tulee dokumentoida sovellettavat valvonta- ja turvatoimet. Vaatimuksiin kuuluu myös erilaiset turvallisuusmenettelyt työsuhteen eri vaiheissa, erityisesti työsuhteen alussa, työtehtävien muutoksissa ja työsuhteen päättyessä. (Katakri 2015, 8-13.)

Toiminnan jatkuvuus tulee varmistaa suunnitteluvaiheessa. Jatkuvuussuunnitelmiin tulee sisällyttää ehkäiseviä ja korjaavia toimenpiteitä, jotta merkittävien toimintahäiriöiden ja poikkeustilanteiden vaikutukset minimoidaan. Suunnitelmissa otetaan myös huomioon salassa pidettävän tiedon suojaaminen poikkeustilanteissa. Organisaation tulee nimetä vastuuhenkilöt tai -tahot, joille poikkeustilanteista tulee ilmoittaa. (Katakri 2015, 10-11.)

Kaikki käsiteltävät tiedot on luokiteltava lakisääteisten vaatimusten mukaan. Salassa pidettävät tiedot merkitään suojaustasoaan kuvaavalla merkinnällä. Jos asiakirja sisältää eri suojaustasoa vaativia tietoja, koko asiakirja merkitään ylimmän suojaustason mukaan. Salassa pidettävien tietojen käsittelijöiden luotettavuus tulee selvittää asianmukaisen tason turvallisuusselvitysmenettelyin. Käsittelijöiden on myös noudatettava salassapito- ja vaitiolokäytäntöjä. (Katakri 2015, 12-13.)

Organisaatiossa tulee ylläpitää rekisteriä salassa pidettävän tiedon käsittelyä edellyttävistä työtehtävistä ja käsittelyoikeuksista suojaustasoittain (Katakri 2015, 15).

4.3.2 Fyysinen turvallisuus

Fyysisen turvallisuuden tarkoituksena on varmistaa, että salassa pidettävät tiedot ovat suojassa oikeudettomalta paljastumiselta. Turvatoimien tarkoituksena on estää salaa tai väkisin tunkeutuminen, ehkäistä, havaita, ja estää luvattomat toimet sekä mahdollistaa henkilöstön luokitus ja pääsy salassa pidettäviin tietoihin heidän tarpeensa mukaan. Turvatoimet määritetään riskienhallintaprosessin perusteella. (Katakri 2015, 16.)

Fyysinen turvallisuus tulee ottaa huomioon jo tilojen ja rakennusten suunnittelussa ja käytössä. Huomioon on syytä ottaa missä tiloissa tietoja käsitellään, minkä suojaustason tietoja käsitellään, tilojen rakenteet ja omat turvajärjestelyt sekä käytettävät ohjelmistot ja järjestelmät. (Katakri 2015, 16.)

Fyysisen turvallisuuden vaatimuksiin kuuluu esimerkiksi asianmukainen lukitus ja kulunvalvonta tiloissa, joissa käsitellään salassa pidettävää tietoa. Organisaatiolla tulee myös olla selkeästi määritelty hallinnollinen alue, jossa henkilöt ja kulkuneuvot voidaan tarkastaa. Ilman saattajia alueelle pääsee vain henkilö, jolla varmistettu kulkulupa. Myös erillinen turva-alue tulee määritellä erikseen. Turva-alueella tulee olla selkeästi määritellyt ja valvotut rajat, joiden avulla kaikkea kulkua sisään ja ulos alueelle voidaan valvoa. Turva-

alueelle pääsy ilman saattajaa vaatii asianmukaisen turvallisuusselvityksen. Alue pyritään rajaamaan rakenteellisesti riskeihin nähden riittävän suojan takaamiseksi. Alueelle tulee laatia turvallisuusmenettelyt, joissa määritellään korkein suojaustaso, jonka tietoja alueelle käsitellään, käytössä olevat suoja- ja turvallisuustoimenpiteet, henkilöt, joilla on pääsy alueelle ilman saattajaa, saattajiin liittyvät menettelyt sekä muut asianmukaiset toimenpiteet ja menettelyt. Tarvittaessa sovelletaan myös teknisen turva-alueen vaatimuksia. Näihin vaatimuksiin kuuluu murtohälytysjärjestelmä, alueen lukitseminen ja valvominen, alueen avainten valvominen sekä säännölliset tarkastukset ja menettelyt luvattomien yhteyksien ja laitteiden löytämiseksi ja poistamiseksi. (Katakri 2015, 19-20.)

Luvattoman pääsyn estämiseksi kulkuoikeuksien hallinta tulee järjestää niin, että luvaton pääsy tietoihin on estetty. Pääsy tietoihin sallitaan ainoastaan työtehtävien perusteella. (Katakri 2015, 24.)

4.3.3 Tekninen tietoturvallisuus

Teknisen tietoturvallisuuden vaatimuksia soveltamalla pyritään varmistamaan turvallisuusjärjestelyjen riittävyys salassa pidettävän tiedon sähköisissä käyttöympäristöissä. Vaatimukset jaetaan tietoliikenne-, tietojärjestelmä-, tietoaineisto- ja käyttöturvallisuuden osioihin. Osioiden tarkoituksenmukainen käyttö edellyttää kohdistetun riskien arvioinnin pohjalta tapahtuvaa vaatimusten tulkintaa. Organisaation suojausten tulee olla riittäviä sekä organisaation oman, että toimivaltaisen viranomaisen riskienarvioinnin havaintoihin nähden. Kustannusten hallitsemiseksi salassa pidettävät tiedot tulee luokitella tarkoituksenmukaisesti sekä tiedon käsittely-ympäristön tulee rajata mahdollisimman suppeaksi. (Katakri 2015, 29.)

Teknisen tietoturvallisuuden vaatimukset on jaettu suojaustasoihin IV, III ja II (Katakri 2015, 3). Suojaustaso IV vaatii muun muassa sen, että tietojenkäsittely-ympäristö on erotettu muista ympäristöistä tai käytössä on vähintään palomuuriratkaisu. Fyysisen turva-alueen ulkopuolelle menevä liikenne tulee salata kyseiselle suojaustasolle hyväksytyllä salausratkaisulla. Näiden lisäksi suojaustasolla III-II tietojenkäsittely-ympäristön kytkeminen muiden suojaustasojen ympäristöihin edellyttää viranomaisen hyväksymää yhdyskäytäväratkaisua. (Katakri 2015, 30.)

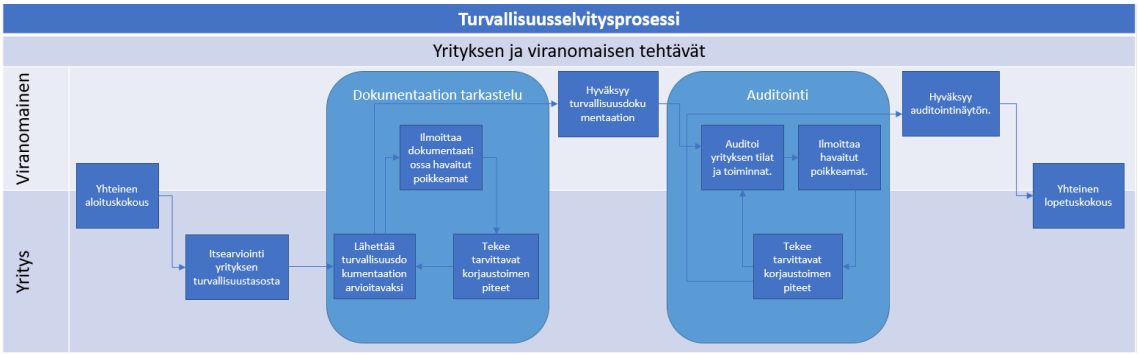
Kaikilla suojaustasoilla vaaditaan, että tietoliikenneverkon vyöhykkeistäminen ja suodattaminen on toteutettu vähimpien oikeuksien ja monitasoisen suojaamisen periaatteiden

mukaan. Vaatimus voidaan täyttää siten, että tietoliikenneverkko on jaettu suojaustason sisällä erillisiin verkko-alueisiin eli vyöhykkeisiin. Vyöhykkeisiin jakaminen tarkoittaa esimerkiksi hankekohtaista työasemien ja palvelimien erottelua. Kaikkea tietoliikennettä on lähtökohtaisesti käsiteltävä epäluotettavana. Vyöhykkeiden välistä liikennettä tulee valvoa ja rajoittaa siten, että vain erikseen hyväksytty liikenne on sallittu. Suodatus- ja valvontajärjestelmien toiminnasta ja tarkoituksenmukaisuudesta huolehditaan ja koko tietojenkäsittely-ympäristön elinkaaren ajan. Järjestelmien tai laitteiden lisäämiseen, muuttamiseen ja poistamiseen tulee määrittää vastuuhenkilöt ja toimintaohjeet. (Katakri 2015, 33-34.)

4.3.4 Katakrin käyttö osana yritysturvallisuusselvitystä

Katakria voidaan käyttää työkaluna yritysturvallisuusselvityksessä, jossa viranomainen selvittää laissa mainittujen tietolähteiden, henkilöturvallisuusselvitysten sekä yritykseen ja sen toimitiloihin kohdistuvan tarkastusten avulla, kykeneekö yritys huolehtimaan tietoturvavelvoitteistaan. Tarkasteltavia turvallisuusjärjestelyjä ovat esimerkiksi salassa pidettävien tietojen suojaaminen, asiattoman pääsyn estäminen tiloihin sekä henkilöstön ohjeistaminen ja kouluttaminen. (Katakri 2015, 66-67.)

Kuvassa 1 on kuvattu Katakrissa määritelty yrityksenturvallisuusselvitysprosessi. Kuvassa käydään läpi yrityksen ja viranomaisen tehtävät.



Kuva 1. Turvallisuusselvitysprosessi.

Turvallisuusselvitys voidaan tarpeen vaatiessa laatia vain osittaisena. Riippuen siitä edellytetäänkö yritykseltä kykyä suojata viranomaisen salassa pidettävää tietoa, käytetään Katakrin eri osa-alueiden eri vaatimuksia tarpeiden mukaan. Ennen arviointia yrityksen tulee suorittaa turvallisuusjärjestelyt ja -riskit sellaiselle tasolle, että ne ovat riskienhallinnassa hyväksyttäviä. Yrityksen tulee toimittaa viranomaiselle riskienhallintatuloksensa sekä kuvaus yrityksen turvallisuusjärjestelyjen vaatimuksenmukaisuudesta. (Katakri 2015, 67.)

4.4 Yhteenveto

Tähän lukuun on koottu taulukkoon aineiston analyysin perusteella keskeisimmät vaatimukset lääkinnällisen ohjelmiston siirtämiselle pilvipalveluun.

Taulukko 2. Yhteenveto lääkinnällisten ohjelmiston oleellisimmista vaatimuksista pilvipalvelussa

Numero	Vaatimus	Lähde
1.	Palvelun omistajan tulee määritellä käsittelyperiaatteet erityisesti tiedonkäsittelylle ei-luotetuissa ympäristöissä, kuten pilvipalveluissa tai asiakkaiden päätelaitteilla	VAHTI-ohje, Sähköisen asioinnin tietoturvallisuusohje
2.	Tietoturvallisuutta koskeviin tehtäviin tulee nimetä vastuuhenkilö.	VAHTI-ohje, Sähköisen asioinnin tietoturvallisuusohje; Katakri
3.	Tietoturvapoikkeamiin ja niistä palautumiseen tulee varautua etukäteen.	VAHTI-ohje, Sähköisen asioinnin tietoturvallisuusohje; Katakri, Turvallisuusjohtaminen
4.	Pilvipalveluiden käyttöä voidaan laajentaa vasta, kun niissä on mahdollista käyttää asiakkaan tarkastamaa ja hyväksymää salausratkaisua.	VAHTI-ohje, Ohje salauskäytännöstä
5.	Organisaation tulee luokitella käyttämänsä tiedot oikeaoppisesti	VAHTI-ohje, Ohje salauskäytännöstä
6.	Tiedot tulee salata tarpeen mukaan	VAHTI-ohje, Ohje salauskäytännöstä
7.	Kaikki käsiteltävät tiedot on luokiteltava lakisääteisten vaatimusten mukaan.	Katakri, Turvallisuusjohtaminen
8.	Tiloissa, joissa käsitellään salassa pidettävää tietoa, on oltava asianmukainen lukitus ja kulunvalvonta	Katakri, Fyysinen turvallisuus
9.	Henkilön tulee antaa suostumus henkilötietojensa keräämiseen ja käsittelyyn selkeästi suostumusta ilmaisevalla toimella	GDPR
10.	Rekisterinpitäjän on toteutettava tarvittavat toimenpiteet, joilla varmistetaan, että henkilötietojen käsittelyssä noudatetaan EU:n tietosuoja-asetusta.	GDPR

Taulukkoon 2 on koottu oleellisimmat vaatimukset lääkkinnällisille ohjelmistoille pilvipalvelussa. Liitteessä 1 oleva taulukko sisältää enemmän vaatimuksia. Taulukon tarkoitus

on antaa organisaatiolle, joka harkitsee lääkinnällisen ohjelmiston kokonaan tai osittain siirtämistä pilvipalveluun, kuva siihen liittyvistä vaatimuksista. Taulukon perusteella organisaatio saa alustavan kuvan pilvipalvelun tuomista vaatimuksista ja voi tehdä oman arvionsa siitä, ovatko pilvipalvelun tuomat hyödyt vaatimusten tuoman lisävaivan arvoista jo ennen varsinaisen päätöksen tekoa ja työn aloittamista. Monet vaatimukset kuitenkin koskevat jo kaikkia organisaatioita, jotka käsittelevät esimerkiksi potilastietoja tai muita salassa pidettäviä tietoja.

5 JOHTOPÄÄTÖS

Monet yritykset haluavat hyödyntää pilviteknologian tuomia mahdollisuuksia. Pilvilaskenta vapauttaa yrityksen palvelimien rakentamisesta, turvallisuudesta ja ylläpidosta.

Yrityksen kannalta pilviteknologian suurin hyöty on vapautuminen fyysisten laitteiden ja turvallisuuden hoitamisesta. Muita hyötyjä ovat esimerkiksi vähentyneet IT-kulut, muokattavuus ja tietoturvallisuus. Pilvipalveluissa palveluntarjoaja ja asiakas jakavat vastuun palvelun ja tietojen turvallisuudesta, mutta koska pilvipalvelussa palvelimet ja tiedot eivät sijaitse fyysisesti organisaation tiloissa, on kiinnitettävä erityistä huomiota tietoturvaan ja palveluntarjoajan luotettavuuteen.

Pilvipalvelun käyttöön liittyy myös riskejä. Helpoin tapa arvioida pilvipalveluun liittyviä riskejä, on hankkia kolmas osapuoli tekemään arviointi. Jos organisaation harkitsee pilvipalvelun käyttämistä, sen on ensin arvioitava turvallissuuteen, yksityisyyteen ja lakien ja säädösten noudattamiseen liittyvät riskit. Organisaation tulisi myös perehtyä omiinsa ja palveluntarjoajan oikeuksiin ja vastuualueisiin pilvipalvelun tietoturvan kannalta.

Aineiston analyysin perusteella voidaan todeta, että lääkinnällisen ohjelmiston siirtäminen pilvipalveluun on mahdollista, jos organisaatio on valmis toteuttamaan kaikki sen tuomat vaatimukset. Organisaatio, joka käsittelee esimerkiksi potilastietoja, henkilötietoja tai muita salassa pidettäviä tietoja, joutuu joka tapauksessa täyttämään suurimman osan näistä vaatimuksista, vaikka se ei käyttäisikään pilvipalvelua. Selkeästi suurin vaikuttaja henkilötietojen käsittelyyn on toukokuussa 2018 voimaan tuleva Euroopan unionin yleinen tietosuoja-asetus, joka vaikuttaa kaikkeen henkilötietojen käsittelyyn koko EU:n alueella.

LÄHTEET

Businnes Queensland. 2017. Benefits of cloud computing. Viitattu 31.5.2018. https://www.business.qld.gov.au/running-business/it/cloud-computing/benefits

Businnes Queensland. 2016. Risks of cloud computing. Viitattu 31.5.2018. https://www.business.qld.gov.au/running-business/it/cloud-computing/risks

Euroopan unionin neuvosto. 1993. Neuvoston direktiivi 93/42/ETY. Viitattu 5.4.2018. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:fi:PDF

Euroopan unionin neuvosto. 2016. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Viitattu 15.4.2018. http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=

Heiser, J & Nicolett, M. 2008. Accessing the Security Risks of Cloud Computing. Viitattu 31.5.2018 https://s3.amazonaws.com/academia.edu.documents/33355553/Gartner_Security_Risks_of_Cloud.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1527766587&Signature=4X6Bok%2BC7r2efqK5g8771J47xlc%3D&response-content-disposition=inline%3B%20filename%3DAssessing_the_Security_Risks_of_Cloud_Co.pdf

Kulkarni S. 2016. Responsibility Of Cloud Service Provider (CSP) And Customer. Viitattu 22.5.2018. https://securitycommunity.tcs.com/infosecsoapbox/articles/2016/12/19/cloud-security-responsibility-cloud-service-provider-csp-and-customer

Mell, P & Grance, T. 2011. The NIST Definition of Cloud Computing. Viitattu 22.3.2018. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Puolustusministeriö. Katakri. 2015. Viitattu 21.3.2018. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Rousku, K. 2017. Sähköisen asioinnin tietoturvallisuus-ohje. Viitattu 9.4.2018. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80012/VM_25_2017.pdf?sequence=1&isAllowed=y

Simorjay F. 2017. Shared Responsibilities for Cloud Computing. Viitattu 23.5.2018. https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91

Search Cloud Computing. 2017. Cloud computing. Viitattu 18.5.2018. https://searchcloudcomputing.techtarget.com/definition/cloud-computing

Tietosuojavaltuutetun toimisto. 2015. EU:n tietosuojauudistus. Viitattu 24.4.2018. http://tietosuoja.fi/fi/index/euntietosuojauudistus.html

Tietosuojatyöryhmä. 2016. Oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevat ohjeet. Viitattu 23.4.2018. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/UpTS0GArv/Oikeus_siirtaa_tiedot_jarjestelmasta_toiseenwp242rev01_fi.pdf

Valtiovarainministeriö. 2015. Ohje salauskäytännöstä. Viitattu 22.4.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=8e28cd10-2e1e-4bd5-b6f1-f75a1fec2f5d&groupId=10229

Valtiovarainministeriö. Voimassa olevat tietoturvaohjeet ja -määräykset. Viitattu 22.4.2018. http://vm.fi/julkaisut/vahti

Valtiovarainministeriö. VAHTI-toiminta. Viitattu 18.4.2018. http://vm.fi/vahti

Valvira. 2009. Käyttötarkoituksen määrittely. Viitattu 5.4.2018. http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/terveydenhuollon_laitteet_ja_tarvikkeet/kayttotarkoituksen_maarittely_ja_luokittelu

Valvira 2017. Terveydenhuollon laitteet ja tarvikkeet. Viitattu 3.4.2018. http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/terveydenhuollon_laitteet_ja_tarvikkeet

Numero	Vaatimus	Lähde
1.	Palvelun omistajan tulee määritellä käsittelyperiaatteet erityisesti tiedonkäsittelylle ei-luotetuissa ympäristöissä, kuten pilvipalveluissa tai asiakkaiden päätelaitteilla	VAHTI-ohje, Sähköisen asioinnin tietoturvallisuusohje
2.	Palvelun omistajan tulee tunnistaa palvelun käyttötilanteet ja tietää missä laajuudessa ja missä tietoverkoissa salassa pidettävää tietoa käsitellään	VAHTI-ohje, Sähköisen asioinnin tietoturvallisuusohje
3.	Palvelun suunnittelussa tulee soveltaa ratkaisuja, jotka rajaavat pääsyä salassa pidettäviin tietoihin käyttäjien tarpeiden mukaan	VAHTI-ohje, Sähköisen asioinnin tietoturvallisuusohje
4.	Tietoturvallisuutta koskeviin tehtäviin tulee nimetä vastuuhenkilö.	VAHTI-ohje, Sähköisen asioinnin tietoturvallisuusohje; Katakri
5.	Omistajan tulee arvioida palveluun kohdistuvia uhkia ja niiden vaikutuksia sekä varmistaa riittävä tietoturvan taso ja vaatimuksenmukaisuus	VAHTI-ohje, Sähköisen asioinnin tietoturvallisuusohje; Katakri
6.	Jo suunnitteluvaiheessa tulee varmistaa, että palvelun tapahtumista kerätään riittävät lokitiedot ja, että lokitiedot ovat tarvittaessa palvelun omistajan saatavilla.	VAHTI-ohje, Sähköisen asioinnin tietoturvallisuusohje
7.	Tietoturvapoikkeamiin ja niistä palautumiseen tulee varautua etukäteen.	VAHTI-ohje, Sähköisen asioinnin tietoturvallisuusohje; Katakri, Turvallisuusjohtaminen
8.	Pilvipalveluiden käyttöä voidaan laajentaa vasta, kun niissä on mahdollista käyttää asiakkaan tarkastamaa ja hyväksymää salausratkaisua.	VAHTI-ohje, Ohje salauskäytännöstä
9.	Organisaation tulee luokitella käyttämänsä tiedot oikeaoppisesti	VAHTI-ohje, Ohje salauskäytännöstä
10.	Tiedot tulee salata tarpeen mukaan	VAHTI-ohje, Ohje salauskäytännöstä
11.	Erityistä huolellisuutta tulee noudattaa kansainvälisten salassa pidettävien tietojen käsittelyssä	VAHTI-ohje, Ohje salauskäytännöstä
12.	Tarpeet ja vaatimukset salaustuotteille tulee määrittää	VAHTI-ohje, Ohje salauskäytännöstä
13.	Salaustuote tulee ottaa käyttöön oikeaoppisesti	VAHTI-ohje, Ohje salauskäytännöstä
14.	Avaintenhallinta tulee suunnitella ja toteuttaa huolellisesti	VAHTI-ohje, Ohje salauskäytännöstä
15.	Salausjärjestelmien varmenteet tulee hallita ja uusia ajallaan	VAHTI-ohje, Ohje salauskäytännöstä
16.	Kiintolevyt tulee salata	VAHTI-ohje, Ohje salauskäytännöstä
17.	Tietoturvakokonaisuus tulee auditoida säännöllisesti	VAHTI-ohje, Ohje salauskäytännöstä
18.	Suojaratkaisu tulee toteuttaa monikerroksisesti	VAHTI-ohje, Ohje salauskäytännöstä
19.	Organisaation tulee nimetä vastuuhenkilöt tai tahot, joille poikkeustilanteista tulee ilmoittaa.	Katakri, Turvallisuusjohtaminen
20.	Kaikki käsiteltävät tiedot on luokiteltava lakisääteisten vaatimusten mukaan.	Katakri, Turvallisuusjohtaminen

21.	Salassa pidettävät tiedot merkitään suojaustasoaan kuvaavalla merkinnällä. Jos asiakirja sisältää eri suojaustasoa vaativia tietoja, koko asiakirja merkitään ylimmän suojaustason mukaan.	Katakri, Turvallisuusjohtaminen
22.	Organisaatiossa tulee ylläpitää rekisteriä salassa pidettävän tiedon käsittelyä edellyttävistä työtehtävistä ja käsittelyoikeuksista suojaustasoittain.	Katakri, Turvallisuusjohtaminen
23.	Tiloissa, joissa käsitellään salassa pidettävää tietoa, on oltava asianmukainen lukitus ja kulunvalvonta	Katakri, Fyysinen turvallisuus
24.	Tiloihin, joissa käsitellään salassa pidettävää tietoa, pääsy ilman saattajaa vaatii asianmukaisen turvallisuusselvityksen	Katakri, Fyysinen turvallisuus
25.	Fyysisen turva-alueen ulkopuolelle menevä liikenne tulee salata kyseiselle suojaustasolle hyväksytyllä salausratkaisulla.	Katakri, Tekninen tietoturvallisuus
26.	Kaikilla suojaustasoilla vaaditaan, että tietoliikenneverkon vyöhykkeistäminen ja suodattaminen on toteutettu vähimpien oikeuksien ja monitasoisen suojaamisen periaatteiden mukaan	Katakri, Tekninen tietoturvallisuus
27.	Vyöhykkeiden välistä liikennettä tulee valvoa ja rajoittaa siten, että vain erikseen hyväksytty liikenne on sallittu.	Katakri, Tekninen tietoturvallisuus
28.	Suodatus- ja valvontajärjestelmien tai laitteiden lisäämiseen, muuttamiseen ja poistamiseen tulee määrittää vastuuhenkilöt ja toimintaohjeet.	Katakri, Tekninen tietoturvallisuus
29.	Henkilön tulee antaa suostumus henkilötietojensa keräämiseen ja käsittelyyn selkeästi suostumusta ilmaisevalla toimella	GDPR
30.	Henkilöille tulee läpinäkyvästi kertoa, miten heidän tietojaan kerätään ja käytetään.	GDPR
31.	Tietojen käsittelyn tarkoitukset on määritettävä ja ilmoitettava kyseiselle henkilölle tietojen keruun yhteydessä.	GDPR
32.	Omistajan on voitava osoittaa henkilön antama suostumus.	GDPR
33.	Jos suostumus annettaan jotakin muuta koskevan ilmoituksen yhteydessä, tulee varmistaa, että henkilö on tietoinen antamastaan suostumuksesta ja siitä mitä suostumus kattaa.	GDPR
34.	Rekisterinpitäjän tulee viipymättä ilmoittaa henkilötietojen tietoturvaloukkauksesta kyseiselle henkilölle. Ilmoituksessa tulee kuvata tietoturvaloukkauksen luonne ja suositeltava toimenpiteitä	GDPR
35.	Rekisterinpitäjän on toteutettava tarvittavat toimenpiteet, joilla varmistetaan, että henkilötietojen käsittelyssä noudatetaan EU:n tietosuoja-asetusta.	GDPR
36.	Tietojen käsittely on määritettävä sopimuksella tai muulla oikeudellisella asiakirjalla, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa määritellään käsittelyn kohde, kesto ja tarkoitus.	GDPR
37.	Henkilötietojen käsittelijä sitoutuu noudattamaan salassapitovelvollisuutta	GDPR; Katakri, Turvallisuusjohtaminen
38.	Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot jäsennellyssä muodossa ja tallentaa ne henkilökohtaista käyttöä varten sekä siirtää kyseiset tiedot toiselle rekisterinpitäjälle.	GDPR, Oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevat ohjeet